

EQUIPMENT AND SYSTEM FOR CIPHER COMMUNICATION AND CIPHERING DEVICE

Patent number: JP9018469
Publication date: 1997-01-17
Inventor: YAMAMOTO TAKAHISA
Applicant: CANON INC
Classification:
- **international:** H04L9/16; H04L9/22
- **European:**
Application number: JP19950165932 19950630
Priority number(s):

Abstract of JP9018469

PURPOSE: To set the proper ciphering system by a transmitter and a receiver in a ciphering communication network.

CONSTITUTION: A terminal 10 for communication is provided with ciphering devices 11 performing ciphering and decoding which are different in ciphering systems, a selection means 14 selecting one of the ciphering devices 11 and a key generation/selector 13 generating the ciphering key according to the selection. The ciphering system which is suitable for the communication is discussed, determined and selected with the terminal 10 for communication on an opposite side. Therefore, the ciphering system having the ciphering intensity according to the secrecy required for information to be communicated is set.

Data supplied from the **esp@cenet** database - Patent Abstracts of Japan

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-18469

(43)公開日 平成9年(1997)1月17日

(51)Int.Cl.⁶
H 0 4 L 9/16
9/22

識別記号

府内整理番号

F I
H 0 4 L 9/00

技術表示箇所
6 4 3
6 5 5
C5-6

審査請求 未請求 請求項の数9 OL (全14頁)

(21)出願番号 特願平7-165932

(22)出願日 平成7年(1995)6月30日

(71)出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72)発明者 山本 貴久

東京都大田区下丸子3丁目30番2号 キヤノン株式会社内

(74)代理人 弁理士 國分 孝悦

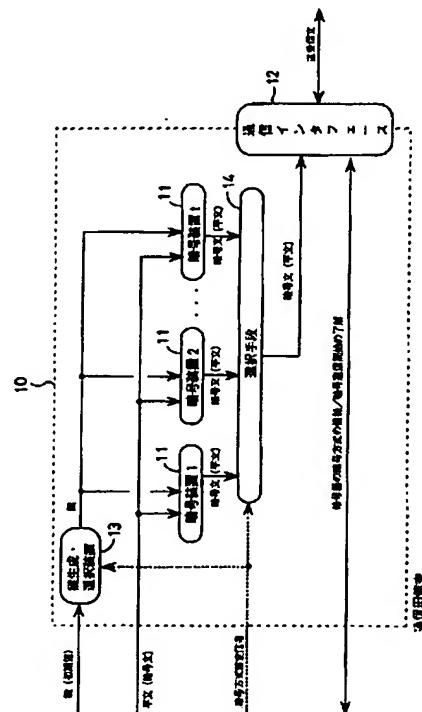
(54)【発明の名称】 暗号通信装置、システム及び暗号装置

(57)【要約】

【目的】 暗号通信ネットワークにおいて送受信者が適切な暗号方式を設定できるようにする。

【構成】 通信用端末10には、それぞれ暗号方式の異なる暗号化及び復号を行う暗号装置11、暗号装置11の1つを選択する選択手段14、その選択に応じて暗号の鍵を生成する鍵生成・選択装置13が設けられ、相手側の通信用端末10とその通信に適した暗号方式を互いに打合わせをして決定し、選択できるようにする。

【効果】 通信する情報に要求される機密性に応じた暗号強度を有する暗号方式を設定することができる。



【特許請求の範囲】

【請求項1】 それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、

上記通信手段に設けられ、複数の暗号化方式の1つを選択する選択手段とを備えた暗号通信装置。

【請求項2】 上記通信手段に設けられ、上記選択手段が選択した暗号化方式に対応した鍵を生成する鍵生成手段を備えた請求項1記載の暗号通信装置。

【請求項3】 上記通信手段に設けられ、上記送信データの暗号化処理時に上記鍵生成手段で生成される鍵を随時更新させる更新手段を備えた請求項2記載の暗号通信装置。

【請求項4】 上記通信手段に設けられ、上記選択手段が選択する暗号化方式を、互いに通信を行うことにより決定する決定手段を備えた請求項1記載の暗号通信装置。

【請求項5】 上記鍵生成手段で用いるアルゴリズムとして、計算量的に安全な疑似乱数生成のアルゴリズムを用いることを特徴とする請求項2記載の暗号通信装置。

【請求項6】 上記計算量的に安全な疑似乱数生成アルゴリズムとして2乗型疑似乱数生成アルゴリズムを用いることを特徴とする請求項5記載の暗号通信装置。

【請求項7】 複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

動作モードを指定するモード指定手段とを備え、

上記暗号化手段は、指定されたモードに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項8】 複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、

セキュリティランクを指定する指定手段とを備え、

上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択することを特徴とする暗号装置。

【請求項9】 ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とすることを特徴とする暗号通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、データを秘匿するためにデータを暗号化して通信を行う暗号通信装置、システム及びそれに用いる暗号装置に関するものである。

【0002】

【従来の技術】 近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛生通信の実用化、ローカルエアリネットワークの普及等に伴い、かかる通信網を利用して様々な情報をやり取りすることが実現されようとしている。加えて、その情報

として動画像データ、静止画像データ、音声データ、コンピュータデータ等のマルチメディア情報を伝送することが考えられている。このような通信網においては、情報を安全に伝達することが重要であり、そのための手段として種々の暗号が知られている。それらの暗号は大きく分けて、共通鍵暗号と公開鍵暗号との2つ暗号方式に分類されるが、それぞれの分類に対して種々の方式が考えられている。

【0003】 図14は共通鍵暗号通信ネットワーク、図15は公開鍵暗号通信ネットワークを示す。図16は共通鍵、公開鍵暗号ネットワークを示し、図14の共通鍵暗号通信ネットワークに図15の公開鍵暗号通信ネットワークを付加した構成になっている。

【0004】 まず、共通鍵暗号方式による暗号通信について述べる。共通鍵暗号通信ネットワークでは、図14に示すように、あらかじめネットワークの加入者間で固有かつ秘密の鍵を共有している。A、B、C、…、Mはそのネットワークの加入者、 K_{AB} 、 K_{AC} 、…はそれぞれ加入者A-B間で共有している鍵、加入者A-C間で共有している鍵、…を示している。さらにそれぞれの加入者は、図17に示すような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者AからBへの共通鍵暗号通信は以下の手順で行う。

【0005】 1. Aは、あらかじめ送信先Bと共有している秘密の鍵 K_{AB} を本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものBに送信する。

2. Bはあらかじめ送信元Aと共有している秘密の鍵 K_{AB} を本通信の暗号装置の鍵として用いて暗号装置によりAからの受信文を復号し、通信文を得る。

【0006】 次に、公開鍵暗号方式による暗号通信について述べる。図15に示すように、公開鍵暗号通信ネットワークの電子掲示板には、各加入者の公開鍵が加入者のID（名前等）と対応がとれる形で掲示されている。図15においては、加入者A、B、…、Mの公開鍵を K_A^p 、 K_B^p 、…、 K_M^p で示している。また各加入者は自分の公開鍵に対応した秘密鍵を秘密に保有する。図15においては、加入者A、B、…、Mの秘密鍵を K_A^s 、 K_B^s 、…、 K_M^s で示している。さらにそれぞれの加入者は、図17に示されるような、ネットワークで決められたアルゴリズムに従って暗号化（及び復号）を行う暗号装置を備えた通信用端末を持っている。従来の加入者AからBへの公開鍵暗号通信は以下の手順で行う。

【0007】 従来の加入者AからBの公開

1. Aは送信先Bの公開鍵 K_B^p を本通信の暗号装置の鍵として用いて暗号装置により通信文を暗号化し、その暗号化したものBに送信する。

2. Bは、自分の秘密鍵 K_B^s を本通信の暗号装置の鍵

として用いて暗号装置によりAからの受信文を復号し、通信文を得る。これらの手順により暗号通信が行われる。

【0008】以上述べたように、信頼できる通信を実現するために必要な技術である暗号技術に関し、現在のところ知られている代表的な暗号方式に限っても種々の方式が考えられている。また、同じ暗号方式でもいろいろな使用モードが考えられており、さらに暗号解読に対して強度を増すように、いろいろな対策が考えられている。

【0009】ここで、従来の暗号方式としてDES暗号について簡単に説明する。DES暗号では、64ビットのデータブロックを単位に暗号化及び復号が行われ、鍵の長さは56ビット(8ビットのパリティビットを加えると64ビット)とされている。暗号アルゴリズムは転置式と換字式とを基本としており、これらの転置と換字を適当に組み合わせた処理を16段繰り返すことにより、平文のビットパターンをかき混ぜ、意味の分からぬ暗号文に変換している。復号する場合は、逆にかき混ぜることにより、元の平文を復元する。

【0010】このかき混ぜかたのパラメータを56ビットの鍵で指定する。鍵の候補の数は2の56乗(約10の17乗)個であり、総当たりの解読、つまり入手した暗号文と平文のペアに対し、鍵を1回ずつ変化させてチェックする解読を行うと、1回のチェックに500nsかかるとすると(128Mbpsの処理速度)、全体で1000年程度かかる計算になる。

【0011】DESの暗号化処理では、まず64ビットの平文に対して転置(初期転置IP)が行われる。この初期転置は固定である。この転置処理の出力は途中複雑な16段の暗号化処理を経た後に最後に転置(最終転置IP⁻¹)が行われる。この最終転置も固定である。

【0012】初期転置が行われた64ビットのデータは、32ビットずつ左右に分割され左半分がL₀、右半分がR₀となる。このL₀とR₀からL₁とR₁になるまで16段にわたって図18に示す処理が行われる。つまり、n段目の処理を終了したときの左右の32ビットをそれぞれL_n、R_n。すると、L_n、R_nは次式で表されるものとなる。

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \# f(R_{n-1}, K_n)$$

【0014】ここで、#はビット毎のmod2の排他的論理和を意味し、K_nはn段目に入力される48ビットの鍵、L_{n-1}とR_{n-1}はそれぞれn-1段目の出力、fはR_{n-1}とK_nを用いて32ビットのデータを出力する関数である。

【0015】

【発明が解決しようとする課題】しかしながら、従来の暗号通信においては、送信側と受信側でどの暗号方式や使用モードを使用し、また暗号解読に対してどのような

対策を施した方式を使用して暗号通信を行うのかという調整に関しては考慮されていなかった。そのため、送信者と受信者で複数の暗号方式を実行できる暗号装置を持つ場合や、複数の使用モードが実行できる場合に、どのようにして送受信者間で調整を行うことにより、暗号通信を行うのか、あるいは両者の共通の暗号方式を検知して、その暗号方式により暗号通信を行う、というようなことができなかった。

【0016】さらに、やり取りする情報の種類に応じて、送信側と受信側とで暗号方式を打ち合わせるなどの調整に関しては考慮されていなかった。特に、やり取りする情報の種類に応じて暗号の強度を調整することに関しては考慮されていなかった。例えば、やり取りする情報が機密性の高い情報であれば従来の技術で述べたような暗号解読に対し対策を施した方式を用いて安全性の高い暗号通信を行い、やり取りする情報が機密性の高い情報でなければ、通常の暗号方式を用いることにより、暗号装置の負荷を軽減する、というようなことができなかった。従来の暗号通信においては、以上のような問題があった。

【0017】本発明は、上記の問題点を解決するために成されたもので、暗号方式を選択できる暗号通信装置、システム及び暗号装置を得ることを目的としている。

【0018】

【課題を解決するための手段】請求項1の発明においては、それぞれ送信データの暗号化及び受信暗号化データの復号を行い、互いに通信を行う複数の通信手段と、上記通信手段に設けられ、複数の暗号化方式の1つを選択する選択手段とを設けている。

【0019】請求項7の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、動作モードを指定するモード指定手段とを備え、上記暗号化手段は、指定されたモードに応じて暗号化方式を選択する。

【0020】請求項8の発明においては、複数の暗号化方式を選択的に用いて情報を暗号化する暗号化手段と、セキュリティランクを指定する指定手段とを備え、上記暗号化手段は、指定されたセキュリティランクに応じて暗号化方式を選択する。

【0021】請求項9の発明においては、ネットワーク上の複数端末間で暗号化されたデータの通信を行うとともに、暗号化方式を選択し得るようにした暗号通信システムであって、所定の端末装置により指定された暗号化方式を他の端末装置により変更する場合に、上記所定の端末装置側の承諾を必要とする。

【0022】

【作用】本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を任意に設定できると共に、その設定した暗号方式を暗号文の送信に先立って送受信

者間で共有することにより、従来考慮されていなかった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。また、暗号強度の選択も可能にしている。

【0023】

【実施例】以下に実施例1～8を示すが、各実施例は次に示すような観点から成り立っている。

【実施例1】複数の暗号の中から暗号方式を設定する。

【実施例2】共通鍵暗号と公開鍵暗号の中から暗号方式を設定する。 10

【実施例3】複数のブロック暗号の中から暗号方式を設定する。

【実施例4】DES型暗号に対し、複数のf関数を用意し、それらを選択することにより、暗号方式を設定する。

【0024】【実施例5】ブロック暗号に対し、使用モードの中から暗号方式を設定する。

【実施例6】「鍵を更新しながら暗号化を行う」複数の暗号方式の中から暗号方式を設定する。 20

【実施例7】ブロック暗号に対し、「固定の鍵を用いて暗号化を行う」暗号方式と、「鍵を更新しながら暗号化を行う」暗号方式の中から暗号方式を設定する。

【実施例8】実施例7の「鍵を更新しながら暗号化を行う」暗号方式の鍵生成・選択装置の内部変数を読み出し可能にする。

【0025】ただし、本発明の本質は、複数の暗号方式の中から特定の暗号方式を実行できるように選択する手段を有することにある。また、それによって暗号の強度を選択できるようにしたことがある。従って、選択される複数の暗号方式としては、実施例に示した暗号方式に限定されるものではない。従来の技術でも述べたが、現在提案されている暗号方式は多数存在するため、その全ての暗号方式について実施例で示すことは困難である。また、複数の暗号方式を組み合わせたような暗号方式も、本発明により選択される暗号方式として含まれる。 30

【0026】【実施例1】本実施例では、図1に示すように、暗号化（及び復号）を行う複数の暗号装置11と、通信インターフェース12と、鍵生成・選択装置13と、複数の暗号装置11の出力の中から1つを選択する選択手段14とを備えた通信用端末10を用いて暗号通*

$$x_{im} = f(x_i) \quad (i = 0, 1, \dots)$$

$$b_{im} = g(x_{im}) \quad (i = 0, 1, \dots)$$

【0032】鍵生成・選択装置13は、図2に示すように、式(1)のフィードバック演算を行う処理回路13aと、式(2)の演算を行う処理回路13bと、暗号方式設定信号で選択された暗号方式に対応した鍵に必要な長さの出力が、式(2)の演算を行う処理回路13bから出されたときにそれを鍵に変換する演算器13cとから構成される。

* 信を行う。

【0027】各々の暗号装置11は、それぞれ異なる暗号方式の処理を実現する。本実施例では暗号方式として、

- ・暗号方式1
- ・暗号方式2
- ・…
- ・暗号方式t

のt種類の暗号とし、それぞれ暗号装置1、暗号装置2、…、暗号装置tの各暗号装置11でその処理が実現されているとする。さらに、どの暗号装置11を使用するかを暗号方式設定信号により設定できる。尚、以下の説明では、暗号装置11を必要に応じて暗号装置1…tと呼ぶものとする。

【0028】選択手段14は、暗号方式設定信号によって制御され、複数の暗号装置11の出力の中から1つ選択することができる。例えば、暗号方式1の暗号処理を行いたい場合には、暗号方式設定信号によって選択手段14を暗号装置1からの出力を選択するように設定すればよい。同様に暗号方式2の暗号処理を行いたい場合には暗号方式設定信号によって選択手段14を暗号装置2からの出力を選択するように設定すればよい。

【0029】通信インターフェース12は、暗号方式を示す情報と暗号装置11で暗号化された送信文とを伝送路に送信するとともに、通信相手からの暗号方式を示す情報と暗号装置11で暗号化された送信文とを伝送路から受信するための通信インターフェースである。

【0030】さらに、一般に暗号方式毎に鍵の長さは異なっているため、暗号方式設定信号によって選択された暗号方式に対応した鍵を生成、または選択する手段として鍵生成・選択装置13がある。鍵生成・選択装置13では、ある長さを持つ1つの鍵から選択された暗号方式に対応した鍵を生成する。あるいはあらかじめ暗号装置で実現できる暗号方式の数だけ対応する鍵を用意しておき、選択された暗号方式に対応した鍵を選択する。

【0031】図2に本発明による鍵生成・選択装置13の一例を示す。鍵生成・選択装置13は、次に示すようなアルゴリズムに従って鍵を生成する。鍵生成・選択装置13に入力されるある長さを持つ1つの鍵は、以下のアルゴリズムで初期値(x₀)として用いられる。

$$\dots \dots \dots \quad (1)$$

$$\dots \dots \dots \quad (2)$$

【0033】演算器13cでは、式(2)の演算を行う処理回路13bから出力されるb₁、b₂、…、b_tを暗号方式設定信号で選択された暗号方式に対応した長さの鍵に変換することを行う。鍵は選択された暗号方式のアルゴリズムで定められた長さのビット列であり、演算器13cによって例えばb₁、b₂、…、b_tをそのまま並べることにより、あるいはその順序を並び変えるこ

とにより生成される。

【0034】従って、鍵生成・選択装置13の動作は以下のようになる。

1. 初期値として x_0 を、鍵生成・選択装置13に入力する。
2. 式(1)により、 x_1, x_2, \dots, x_n を生成する。
3. 生成された x_1, x_2, \dots, x_n に対して式(2)を実行し、得られた b_1, b_2, \dots, b_n を出力する。
4. 演算器13cにより b_1, b_2, \dots, b_n を暗号方式設定信号で選択された暗号方式に対応した鍵として出力する。

【0035】鍵生成・選択装置13は、暗号方式設定信号によって、式(1)及び式(2)の演算を何回行うか、さらに演算器13cからどれだけの長さの鍵を出力するか、を制御され、そのことにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を生成する。

【0036】また、鍵生成・選択装置13は図3のよう構成することも可能である。図3の鍵生成・選択装置13はt個の鍵(k_1, k_2, \dots, k_t)と鍵選択手段13dとから構成される。鍵 k_1, k_2, \dots, k_t は鍵選択手段13dに入力され、暗号方式設定信号によっていずれかが選択される。これにより暗号方式設定信号によって選択された暗号方式に対応した長さを持つ鍵を選択する。

【0037】上記通信用端末10を用いて暗号通信を行う暗号通信ネットワークとしては図14のものを用いる。鍵の共有は、あらかじめネットワークの管理者等が鍵の設定しておくことによって実現できる。あるいは、文献「暗号と情報セキュリティ」(辻井、笠原著、1990年発行、株式会社昭晃社、72~73、97~104項)示されるような公知の鍵共有方式によっても実現できる。

【0038】本発明による加入者AからBへの暗号通信は以下の手順で行われる。以下の説明では、鍵生成・選択装置13としては、図2に示すものであるとし、上記のように、ある長さを持つ1つの鍵から選択された暗号方式に対応した鍵を生成する。

【0039】[本発明による暗号通信の前手順1]

1. 送信者Aは、暗号方式を示す情報を通信インターフェース12を介して受信者Bに送る。
2. 受信者Bは、送信者Aから送られてきた暗号方式を示す情報を情報通信インターフェース12を介して受信し、受信者Bが利用している通信用端末10にある暗号装置11がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インターフェース12を介して送信者Aに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インターフェース12を介して送信者Aに伝える。

3. 上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【0040】上記の前手順1では、暗号方式を示す情報を送信者の方から示したが、逆に次のように受信者の方から示すことも可能である。

[本発明による暗号通信の前手順2]

1. 受信者Bは、情報の提供の要求とその情報を暗号化する時の暗号方式を示す情報を通信インターフェース12を介して送信者Aに送る。

2. 送信者Aは、受信者Bから送られてきた情報の提供の要求と暗号方式を示す情報を通信インターフェース12を介して受信し、送信者Aが利用している通信用端末10にある暗号装置がその暗号方式で処理できることを確認し、暗号通信の開始の了解を通信インターフェース12を介して受信者Bに伝える。その暗号方式で処理することが困難な場合には、可能な暗号方式を通信インターフェース12を介して受信者Bに伝える。

3. 上記手順を送受信者間で暗号方式に関して合意ができるまで繰り返す。

【0041】上の手順は送信者が受信側の設定可能な暗号方式を知らない場合、あるいは受信者が送信側の設定可能な暗号方式を知らない場合に有効な手順である。送信者が受信側で設定可能な暗号方式を知っている場合、又は受信者が送信側の設定可能な暗号方式を知っている場合には、上記の手順1、だけを行って次の暗号通信を開始することが可能である。

【0042】さらに、暗号通信に先立って暗号鍵を送受信者間で交換するような鍵共有方式を行うような暗号通信ネットワークにおいては、鍵共有のプロトコルにおいて、鍵の共有のための情報と共に暗号方式の情報を共有することが可能である。そのような場合には、上記の手順を省略して暗号通信を開始することが可能である。

【0043】上記前手順1、2によれば、送受信者間で暗号方式を調整することができる。また、上記前手順1、2は通信毎に毎回行う必要はない。例えば、あらかじめ暗号方式を送受信者間で打ち合わせておき、その暗号方式で暗号通信を行う場合には必要ない。

【0044】以下、送信者Aと受信者Bとの間で次の手順を続ける。

[本発明によるデータの暗号通信手順(送信者Aに関する)]

1. 暗号方式設定信号により、前手順1、2で決定した暗号方式からの出力が選択されるように選択手段14を設定する。
2. あらかじめ受信者Bと共有している秘密の鍵 K_{AB} を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置11に設定される。
3. 暗号装置11によりデータを暗号化し、選択手段1

4により前手順で決定した暗号装置11から出力される暗号文を選択し、通信インターフェース12を介してBに送信する。

【0045】[本発明によるデータの暗号通信手順(受信者Bに関する)]

1. 暗号方式設定信号により、前手順1、2で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. あらかじめ送信者Aと共有している秘密の鍵 K_{AB} を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵を生成する。生成された鍵は暗号装置11に設定される。

3. 通信インターフェース12を介して伝送路から暗号化データを受信し、暗号装置11によりAから送られてきた暗号化データを復号し、選択手段14により前手順で決定した暗号装置11から出力される平文を選択する。

【0046】また、鍵生成・選択装置13として図3のものを用いることも可能である。その場合には、図14に示された鍵は、複数の鍵を合わせたものを意味する。つまり、加入者AとBの間の鍵 K_{AB} は、暗号方式1を使う時の鍵 K_{AB1} 、暗号方式2を使う時の鍵 K_{AB2} 、…、暗号方式tを使う時の鍵 K_{ABt} からなる。この場合の本発明による加入者AからBへの暗号通信は以下の手順で行われる。ただし、前手順1、2は上記と同じなので省略する。

【0047】[本発明によるデータの暗号通信手順(送信者Aに関する)]

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. あらかじめ受信者Bと共有している秘密の鍵 K_{AB} (K_{AB1} 、 K_{AB2} 、…、 K_{ABt} から構成される)を通信用端末10内の鍵生成・選択装置13に設定し、暗号方式設定信号により、複数の鍵 K_{AB1} 、 K_{AB2} 、…、 K_{ABt} から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置11に設定される。

3. 暗号装置11によりデータを暗号化し、選択手段14により前手順で決定した暗号装置11から出力される暗号文を選択し、通信インターフェース12を介してBに送信する。

【0048】[本発明によるデータの暗号通信手順(受信者Bに関する)]

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. あらかじめ送信者Aと共有している秘密の鍵 K_{AB} (K_{AB1} 、 K_{AB2} 、…、 K_{ABt} から構成される)を通信用端末10内の鍵生成・選択装置13に設定し、暗号方式設定信号により、複数の鍵 K_{AB1} 、 K_{AB2} 、…、 K_{ABt}

K_{ABt} から選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置11に設定される。

3. 通信インターフェース12を介して伝送路から暗号化データを受信し、暗号装置11によりAから送られてきた暗号化データを復号し、選択手段14により前手順で決定した暗号装置11から出力される平文を選択する。

【0049】また暗号通信ネットワークの加入者はそれぞれ、暗号通信するために必要な各ユーザの鍵などの秘密情報を格納するために、図4に示されるような携帯型記憶装置30を保有していてもよい。携帯型記憶装置30には、暗号通信するために必要な各ユーザの秘密情報が格納されており、安全性を考慮して通信用端末10とは別に各ユーザ毎に携帯型記憶装置30を持つような構成にしている。各ユーザ毎に物理的に安全な領域が確保できるなら携帯型記憶装置30は通信用端末10の一部であってもよいが、その場合は各ユーザ毎に暗号通信に使用できる通信用端末10が制限されてしまう。通信用端末10と携帯型記憶装置30とを分離し、通信用端末10には各ユーザの秘密情報を格納しないようにすることで、ユーザはどの通信用端末10でも自分の携帯型記憶装置30を介してそのユーザの秘密情報をやりとりして暗号通信に使用することが可能となり便利である。

【0050】携帯型記憶装置30は、上記通信用端末と安全な通信路を介して情報のやり取りを行えるようになっており、物理的に安全な領域を保持手段30aとして持つ。携帯型記憶装置30を正常に動作させることができるのは正規の所有者だけであり、パスワード等の認証手続きにより正規の所有者が否かを判断する。また、上記の共有鍵のうちその携帯型記憶装置30の所有者に関するものを保持手段30aに保持している。携帯型記憶装置30はICカード等により実現できる。以下に説明する全ての実施例2～8において、この携帯型記憶装置30を用いる場合に関しても本発明の範囲である。

【0051】[実施例2]本実施例では、図5に示すような、暗号化(及び復号)を行う複数の暗号装置15、16と、通信インターフェース12と、鍵生成・選択装置13と、複数の暗号装置15、16の出力の中から1つを選択する選択手段14とを備えた通信用端末10を用いて暗号通信を行う。

【0052】本実施例では、暗号方式を

1. 共通鍵暗号方式の代表としてDES暗号方式(またはFEAL暗号方式)

2. 公開鍵暗号方式の代表としてRSA暗号方式(またはEIGamal暗号方式)の2種類の暗号方式とし、それぞれDES暗号装置(またはFEAL暗号装置)15と、RSA暗号装置(またはEIGamal暗号装置)16とでその処理が実現されているものとする。ただし、ここで例示したDES暗号、FEAL暗号、RSA暗号、EIGamal暗号は、共通鍵暗号或は公開鍵暗号の代表例として挙げただけで、本発明はこれらに限

定されず他の暗号アルゴリズムにも適用可能である。

【0053】図5の通信用端末10をDES暗号方式で使用する場合には、選択手段14ではDES暗号装置15からの出力を選択するようすればよい。図5の通信用端末10をRSA暗号方式で使用する場合には、選択手段14ではRSA暗号装置16からの出力を選択するようすればよい。

【0054】鍵生成・選択装置13、通信インタフェース12、選択手段14は、実施例1と同様のものを用いる。ただし、鍵生成・選択装置13は図3に示されたものを使い、暗号方式設定信号によって選ばれた暗号方式に対応する鍵を選択する。つまり、DES暗号方式が選ばれた場合は、DES暗号用にあらかじめ配布されている鍵を選択し、RSA暗号方式が選ばれた場合は、RSA暗号用に公開されている公開鍵を選択する。

【0055】また、本実施例では、暗号通信ネットワークとしては図16のものを用いる。図16の共通鍵、公開鍵暗号通信ネットワークは図14の共通鍵暗号通信ネットワークに図15の公開鍵暗号通信ネットワーク付加した構成になっている。

【0056】本発明による加入者AからBへの暗号通信は、以下の手順で行われる。ただし、前手順1、2は実施例1と同様である。

【本発明によるデータの暗号通信手順（送信者Aに関する）】

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. 暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{AB}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置15、16に設定される。

3. 暗号装置15、16によりデータを暗号化し、選択手段14により前手順で決定した暗号装置から出力される暗号文を選択し、通信インタフェース12を介してBに送信する。

【0057】【本発明によるデータの暗号通信手順（受信者Bに関する）】

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. 暗号方式設定信号により、共通鍵K_{AB}と公開鍵K^{AB}とから選択された暗号方式に対応した鍵を選択する。選択された鍵は暗号装置15、16に設定される。

3. 通信インタフェース12を介して伝送路から暗号化データを受信し、暗号装置によりAから送られてきた暗号化データを復号し、選択手段14により前手順で決定した暗号装置から出力される平文を選択する。

【0058】この手順により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応 50

じて暗号方式を選択できる。例えば、特に機密性の高いデータの場合には、公開鍵暗号方式を選択し、そうでない場合には、共通鍵暗号方式を選択して処理を簡易にする。というようなことができる。

【0059】【実施例3】本実施例では、図6に示されるような、暗号化（及び復号）を行う複数の暗号装置17、18と、通信インタフェース12と、鍵生成・選択装置13と、複数の暗号装置17、18の出力の中から1つを選択する選択手段14とを備えた通信用端末10を用いて暗号通信を行う。

【0060】本実施例では、暗号方式として

1. DES暗号
2. F E A L暗号

の2種類のブロック暗号とし、それぞれDES暗号装置17と、F E A L暗号装置18とでその処理が実現されるものとする。ただし、ここで例示したDES暗号、F E A L暗号は共通鍵暗号の代表例として挙げただけで、本発明はこれらに限定されず他の暗号アルゴリズムも適用可能である。

【0061】図6の通信用端末10を用いてDES暗号処理を行いたい場合は、選択手段14では常にDES暗号装置17からの出力を選択するようすればよい。また、F E A L暗号処理を行いたい場合は、選択手段14では常にF E A L暗号装置18からの出力を選択するようすればよい。

【0062】鍵生成・選択装置13、通信インタフェース12、選択手段14は、実施例1と同様のものを用いる。また、上記通信用端末10を用いて暗号通信を行う暗号通信ネットワークとしては図14のものを用いる。

そして本実施例による加入者AからBへの暗号通信は実施例1と同様の手順で行われる。

【0063】【実施例4】本実施例では、図7に示すような、暗号化（及び復号）を行う暗号装置19と、通信インタフェース12と、鍵生成・選択装置13とを備えた通信用端末10を用いて暗号通信を行う。また、これまでの実施例1～3で用いている選択手段14は、本実施例では暗号装置19内に含まれている。

【0064】本実施例では、暗号方式としてDES型（インボリューション型）暗号を用いる。その構成要素であるf関数を複数用意し、その中からあるf関数を選択することにより、複数の暗号方式を設定できる。DES型暗号は前述したように同じ処理を繰り返すアルゴリズムであるので、同じ回路で繰り返し処理を行うことが可能である。例えば図18に示されたDES暗号の1段分の1処理単位として回路化すれば、その回路を繰り返し用いることにより、暗号処理を実現できる。

【0065】この場合の暗号装置19は図8のように構成される。図8の暗号装置19は、レジスタ19a、19bと、排他的論理回路19cと、複数のf関数（f₁、f₂、…、f_n）と、複数のf関数の出力から1つ

を選択する選択手段 19 d とから構成される。選択手段 19 d は、暗号方式設定信号によって制御されている。

【0066】複数の f 関数の構成は、例えば f 関数と同じ数の S box の組を用意しておくことにより実現可能である。この場合には、f 関数 f_1 に対しては $S_{11}, S_{12}, \dots, S_{1n}$ の S box を用い、f 関数 f_2 に対しては $S_{21}, S_{22}, \dots, S_{2n}$ の S box を用い、…、というようにすればよい。また、f 関数 f_1 に対しては DES 暗号の f 関数を用い、f 関数 f_2 に対しては F E A L 暗号の f 関数を用い、…、というように、全く異なる暗号の f 関数を用意することによっても実現できる。

【0067】以上説明したような暗号装置 19 を用いて、実施例 1 と同様の手順により暗号通信を行うことが可能である。尚、鍵生成・選択装置 13、通信インターフェース 12 は、実施例 1 と同様のものを用いる。本実施例でも、暗号通信ネットワークとしては図 14 のものを用いる。本実施例により、送受信者間で暗号方式について調整することができる。

【0068】【実施例 5】本実施例では、図 7 に示す通*

$$C_1 = E_1 (M_1 + I_V)$$

$$C_i = E_i (M_i + C_{i-1}) \quad (i = 2, 3, \dots)$$

$$M_1 = D_1 (C_1) + I_V$$

$$M_i = D_i (C_i) + C_{i-1} \quad (i = 2, 3, \dots)$$

$$\dots \dots \dots (3)$$

$$\dots \dots \dots (4)$$

$$\dots \dots \dots (5)$$

$$\dots \dots \dots (6)$$

【0071】この場合の暗号装置 20 は図 9 のように構成される。図 9 の暗号装置 20 は、ブロック暗号器 20 a と、2 つの入力から一方を選択する選択手段 20 b と、ビット毎に排他的論理演算を行う排他的論理回路 20 c とからなる。選択手段 20 b は、暗号方式設定信号によって制御されている。

【0072】この暗号装置 20 を ECB モードで使用する場合には、入力する初期値 I_V として全て 0 のビット列とし、選択手段 20 b では常に初期値 I_V を選択するようにすればよい。また暗号装置 20 を CBC モードで使用する場合には、入力する初期値 I_V として任意のビット列を設定し、選択手段 20 b では初期のブロックを暗号化する時には初期値 I_V を選択するようにし、以降は暗号装置 20 からの出力を選択するようにすればよい。初期値 I_V は通信者間で秘密にする必要はない。

【0073】以上説明したような暗号装置 20 を用いて、実施例 1 と同様の手順により暗号通信を行なうことが可能である。ただし、前手順において、CBC モードを選択した場合には、初期値 I_V を共有する手順が必要となる。例えば、暗号通信を行う前に A から B へ初期値 I_V を送信する手順が必要となる。初期値 I_V は送受信者間で秘密にする必要はないので、暗号化しなくてもよい。また、秘密の鍵 K_a だけでなく、共有した初期値 I_V を通信用端末 10 内の暗号装置 20 に設定しなければならない。

【0074】鍵生成・選択装置 13 通信インターフェース 12 は実施例 1 と同じものを用いる。本実施例でも、暗

* 信用端末 10 と同一構成の通信用端末を用いて暗号通信を行う。ただし、図 7 の暗号装置 19 に代えて図 9 に示すような暗号装置 20 を用いる。また、選択手段は本実施例でも暗号装置 20 内に含まれている。また、本実施例では、暗号方式によって鍵のビット長は変わらないので鍵生成・選択装置 13 は必ずしも必要ではない。

【0069】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を

1. ECB (E l e c t r i c C o d e b o o k) モード

2. CBC (C i p h e r B l o c k C h a i n i n g) モード

のどちらで使用するか暗号方式設定信号により設定できるものとする。

【0070】CBC モードについては後述するが、ここでも簡単に説明しておく。平文を M_i 、暗号文を C_i 、初期値を I_V とし、暗号鍵 K を用いた暗号化を E_i 、復号を D_i とすると CBC モードは次式で表される。

号通信ネットワークとしては図 14 のものを用いる。本実施例により、送受信者間で暗号方式の使用モードを調整することができる。

【0075】【実施例 6】本実施例は、実施例 1 に基づいて暗号方式を改良したものである。本実施例では、実施例 1 と同じく、図 1 に示す通信用端末 10 を用いて暗号通信を行う。

【0076】本実施例が実施例 1 と異なる点は以下の通りである。実施例 1 では暗号装置 11 は複数存在したが、各々の暗号装置 11 に対する鍵は一度の暗号通信を行っている間は固定である。つまり、暗号通信中には鍵が随時変更されるということではなく、暗号通信の始めから終わりまで同一の鍵を用いる。それに対して本実施例では、第 3 者による暗号解読に対して安全性を向上させるために、暗号通信中に鍵を随時変更する。暗号通信中に鍵を随時更新するために、鍵生成・選択装置 13 では暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置 11 の鍵の更新を行う。ただし、鍵の更新は暗号通信の送信者と受信者とで同期をとって行なう必要がある。

【0077】本実施例の鍵生成・選択装置 13 も、実施例 1 の場合と同じく図 2 のように構成される。ただし、本実施例の鍵生成・選択装置 13 では上述のように、暗号通信中も鍵生成を行い、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成される毎に、暗号装置 11 の鍵の更新をする、ということを行なうため、実

施例1の場合と動作が異っている。

【0078】実施例1の場合の鍵生成・選択装置13は、暗号方式設定信号で選択された暗号方式に対応した長さの鍵が生成されればそれ以上動作させる必要はない。それに対して本実施例での鍵生成・選択装置13では、暗号方式設定信号で選択された暗号方式に対応した長さの鍵を次々に生成する必要がある。つまり、本実施例での鍵生成・選択装置13は、実施例1の場合の鍵生成・選択装置13の動作を何度も繰り返し行っている。

【0079】本発明に用いる鍵生成・選択装置13の鍵生成のアルゴリズムは、特に制限を受ける訳ではなく、*

$$x_{i+1} = x_i \text{ mod } N \quad (i = 0, 1, 2, \dots) \quad \dots \dots \dots \quad (7)$$

$$b_i = 1 \text{ s } b_i \quad (x_i) \quad (i = 1, 2, \dots) \quad \dots \dots \dots \quad (8)$$

によって得られるビット系列 b_1, b_2, \dots を2乗型疑似乱数系列という。但し、 $1 \text{ s } b_i \quad (x_i)$ は x_i の下位 j ビットを表わし、 N のビット数を n としたとき $j = O(\log n)$ とする。

【0081】2乗疑似乱数系列は、法 N における平方剰余性の判定問題が計算量的に困難であるとの仮定の下で計算量的に安全な疑似乱数系列となる。2乗疑似乱数を十分安全なものとするため、2乗演算式(7)の法 N のビット数 n を 512 ビット程度とすることが望ましい。さらに、各加入者間であらかじめ秘密に共有されている鍵(鍵生成・選択装置の初期値) K_{AB}, K_{AC}, \dots は、 $1 < K_{AB}, K_{AC}, \dots < N - 1$ とする。

【0082】この2乗疑似乱数系列を用いた鍵生成・選択装置13は図10に示される。図10の鍵生成・選択装置13は式(7)のフィードバック演算を行う処理回路13eと式(8)の演算を行う処理回路13fと演算装置13gとから構成される。この鍵生成・選択装置13の動作は以下のようになる。

1. 初期値 x_0 を鍵生成・選択装置13に入力する。
2. 式(7)により、 x_1, x_2, \dots を生成する。
3. 生成された x_1, x_2, \dots に対し、式(8)を実行し、得られた b_1, b_2, \dots を出力する。
4. 演算器13gでは b_1, b_2, \dots を暗号方式設定信号で選択された暗号方式に対応した長さの鍵の鍵列 k_1, k_2, \dots に変換する。

【0083】図11に鍵を随時更新する場合の暗号通信の図を示す。暗号方式としてブロック暗号を考える。図40において、 M_{uv} ($u = 1, 2, \dots, t; v = 1, 2, \dots, s$) は平文ブロックを、 k_u ($u = 1, 2, \dots, t$) はブロック暗号の鍵を、 k_v (M_{uv}) ($u = 1, 2, \dots, t; v = 1, 2, \dots, s$) は平文ブロック M_{uv} を鍵 k_v で暗号化して得られる暗号文ブロックを示している。ここで、 M_u から M_s までの s 個のブロックは同じ鍵 k_v で暗号化されている。前述の鍵生成・選択装置13によって更新される鍵系列 k_1, k_2, \dots を順にブロック暗号の鍵として用いることにより、図11の平文ブロックは複数の暗号鍵によって暗号化される。こ50

* 実施例1で示したような一般的なものを用いることが可能であるが、本実施例では鍵生成のアルゴリズムとして、計算量的に安全な疑似乱数系列生成アルゴリズムを用いた場合、特にその中でも2乗型疑似乱数系列を用いた場合について説明する。

【0080】2乗型疑似乱数系列とは、以下の手順で生成される疑似乱数系列 b_1, b_2, \dots である。

【2乗型疑似乱数系列】 p, q を $p \equiv q \equiv 3 \pmod{4}$ である素数とし、 $N = p \cdot q$ として、初期値 x_0 ($1 < x_0 < N - 1$ なる整数) と再帰式

$$\dots \dots \dots \quad (7)$$

$$\dots \dots \dots \quad (8)$$

のように随時鍵を更新することにより、同じ鍵で暗号化される平文ブロックの数が s 個になり、鍵の解析を困難にすることができる。尚、本実施例でも、暗号通信ネットワークとしては図14のものを用いる。

【0084】加入者AからBへの暗号通信は、以下の手順で行われる。ただし、前手順は実施例1と同様である。

【本発明によるデータの暗号通信手順(送信者Aに関する)】

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. あらかじめ受信者Bと共有している秘密の鍵 K_{AB} を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

3. 鍵生成・選択装置13から出力される鍵列を暗号装置11の鍵として随時更新しつつ用いデータを暗号化し、選択手段14により前手順で決定した暗号装置11から出力される暗号文を選択し、通信インターフェース12を介してBに送信する。

【0085】【本発明によるデータの暗号通信手順(受信者Bに関する)】

1. 暗号方式設定信号により、前手順で決定した暗号方式からの出力が選択されるように選択手段14を設定する。

2. あらかじめ送信者Aと共有している秘密の鍵 K_{AB} を通信用端末10内の鍵生成・選択装置13に初期値として設定し、暗号方式設定信号で選択された暗号方式に対応した鍵列を生成する。

3. 通信インターフェース12を介して伝送路から暗号化データを受信し、鍵生成・選択装置13から出力される鍵列を暗号装置11の鍵として随時更新しつつ用いて、送られてきた暗号化データを復号し、選択手段14により前手順で決定した暗号装置11から出力される平文を選択する。

【0086】また、計算量的に安全な疑似乱数生成のア

ルゴリズムとして2乗型疑似乱数を用いたが、計算量的に安全な疑似乱数生成アルゴリズムであればどのようなものでも用いることができる。たとえば前記文献「暗号と情報セキュリティ」(辻井、笠原著、1990年発行、株式会社昭晃社、86頁)に示されているように、RSA暗号、離散対数、逆数暗号を用いたものも本発明の疑似乱数生成のアルゴリズムに用いることができる。また、本実施例で説明した鍵を随時更新する方法は、実施例1に基づいて説明したが、実施例1に適用できるだけでなく、実施例3、4、5に対しても適用できる。

【0087】[実施例7] 実施例1は鍵は固定の暗号方式(複数)の中からある暗号方式を選択し、実施例6は鍵は更新される暗号方式(複数)の中からある暗号方式を選択するものである。上記2つの実施例1、6のバリエーションとして本実施例では、鍵は固定の暗号方式と鍵は更新される暗号方式との間で暗号方式を選択できるようにしている。また、本実施例では、図12に示されるような、暗号化(及び復号)を行う暗号装置11と、通信インターフェース12と、鍵生成・選択装置13を備えた通信用端末10を用いて暗号通信を行う。ここで20は、説明の簡単のため暗号装置11は1つであるとする。

【0088】本実施例では、暗号方式としてブロック暗号を考える。さらに、そのブロック暗号を、

1. 固定の鍵を用いて暗号化を行う。
2. 鍵を更新しながら暗号化を行う。

のどちらの方式を使用するか暗号方式設定信号により設定できるものとする。

【0089】鍵生成・選択装置13は暗号方式設定信号によって制御され、「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置13は固定鍵(1つの鍵)を生成すれば処理を停止する。また、「鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、鍵生成・選択装置13は鍵列(複数の鍵)を生成するために処理を繰り返し行う、という動作を行う。図12の通信用端末10を「固定の鍵を用いて暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置13では固定鍵を生成するようにし、暗号装置11ではその固定鍵を用いて暗号化すればよい。また、図12の通信用端末10を「鍵を更新しながら暗号化を行う」暗号方式で使用する場合には、暗号方式設定信号により鍵生成・選択装置13では鍵列を生成するようにし、暗号装置11ではその鍵列により順次鍵を更新しながら暗号化すればよい。鍵生成・選択装置13は図2と同じ構成で動作が実施例6と同じものを用いる。暗号装置11、通信インターフェース12は実施例1と同じものを用いる。また、暗号通信ネットワークとしては図14のものを用いる。

【0090】加入者AからBへの暗号通信は、実施例1と同様の手順で行われる。ただし、鍵を更新しながら暗50

号化を行うことを選択した場合には、データの暗号通信手順は実施例6と同様の手順で行われる。

【0091】本実施例により、送受信者間で暗号方式について調整することができ、暗号通信の安全性を選択することができる。つまり、送信するデータの機密性に応じて暗号方式を選択できる。例えば、特に機密性の高いデータの場合には、「鍵を更新しながら暗号化を行う」暗号方式を選択し、そうでない場合には、「固定の鍵を用いて暗号化を行う」暗号方式を選択して処理を簡易にする、というようなことができる。尚、本実施例では説明の簡単のため、暗号装置11は1つとしたが、複数の暗号装置11を用いてもよい。その場合には、複数の暗号装置11からの出力を選択するための選択手段14が必要となる。

【0092】[実施例8] 本実施例は、実施例6、7で用いた鍵生成・選択装置13の構成を少し変えた場合である。実施例6、7では、各加入者間で共有されている鍵が固定のため、「鍵を更新しながら暗号化を行う」暗号方式においても、送受信者が同じ場合には鍵生成・選択装置13の初期値は常に同じ値となり、同じ鍵列が生成されるという問題がある。

【0093】そこで本実施例では、送受信者が同じでも鍵生成・選択装置13の初期値を利用する毎に変更するようにして安全性を向上させようとしている。

【0094】実施例6に示された鍵列生成の手順である式(7)、式(8)において、フィードバック演算により次々更新される x_{in} を、鍵生成・選択装置13の内部変数と呼ぶことにする。本実施例の鍵生成・選択装置13は、図13に示されるように式(7)のフィードバック演算を行う処理回路13hと式(8)の演算を行う処理回路13iと、演算器13jとから構成され、さらに式(7)の演算により更新される内部変数を読み出せる構成になっている。読み出された内部変数は、例えば実施例1で説明したような通信用端末10に接続された携帯型記憶装置30の保持手段30aに記憶される。

【0095】実施例6、7では、鍵生成・選択装置13へ初期値を設定するだけでデータの移動は一方向であるが、本実施例では逆方向に鍵生成・選択装置13の内部変数の読み出しが行えるようになっている。読み出した内部変数は、次の暗号通信に用いられる共通鍵として、今回の暗号通信に用いた共通鍵に対し置き換えが行われる。

【0096】また、この鍵生成・選択装置13を図10の鍵生成・選択装置13に置き換えることにより、鍵生成・選択装置13の初期値を利用する毎に変更できる通信用端末10を構成できる。

【0097】加入者AからBへの暗号通信は、実施例6、7で示した手順と同様の手順で行われる。ただし、「鍵を更新しながら暗号化を行う」暗号方式の場合には、送受信者双方に「暗号化データの復号が終了した時

の鍵生成・選択装置の内部変数の値を次回A(又はB)と暗号通信するための新しい初期値として携帯型記憶装置の保持手段に秘密に保持する」という手順が最後に必要となる。

【0098】上述の各実施例は、暗号方式設定信号に基づいていずれかの暗号方式を選択的に用いるように構成される。ここで、上述の暗号方式設定信号は、送信者が任意に選択してもよいし、送信されるデータの種類に応じて自動的にいずれかの暗号方式を選択するようにしてもよい。さらに、送信者が送信内容のセキュリティランクを指定する場合には、指定されたセキュリティランクに応じた強度を有する暗号方式を自動的に設定するようにしてもよい。また、上記暗号方式設定信号は、送信者A、B間での動作モード、すなわち送信者A、Bとの間の通信が、例えばTV会議を行うモードや親展通信を行うモード等、に応じて自動的に暗号強度を変えるようにしてもよい。さらに、上記暗号方式の設定は、データを通信する者が優先的に設定してもよいし、両送信者から自由に設定し得るようにもよい。但し、暗号強度を弱くする場合には、相手方の承諾を必要とし、その承諾を得るために交渉を行う通信を行うことが好ましい。また、さらに相手側の復号能力に応じて暗号化方式を設定するようにしてもよい。

【0099】

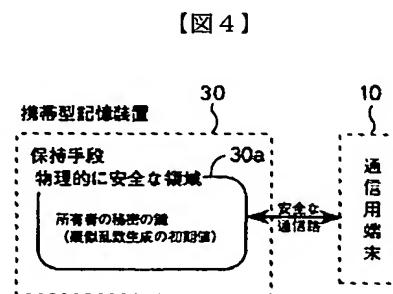
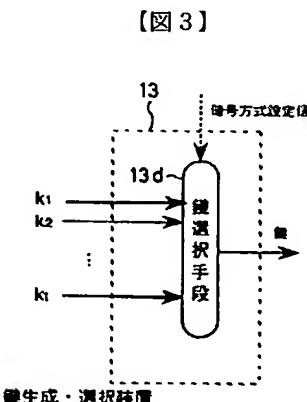
【発明の効果】以上説明したように、本発明によれば、暗号通信を行う送受信者の利用する通信手段に、暗号方式を選択できる選択手段を設けることにより、暗号方式を変更できるようにし、さらにその選択した暗号方式を暗号文の送信に先立って送受信者間で共有することにより、従来不可能であった暗号方式の選択を可能にし、自由度の高い暗号通信を可能にしている。

【図面の簡単な説明】

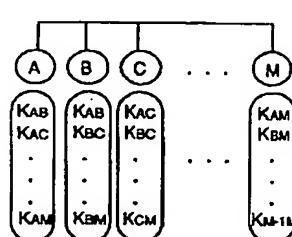
【図1】本発明の実施例1、6による通信用端末のブロック図である。

【図2】本発明の実施例1、6、7による鍵生成・選択装置のブロック図である。

【図3】本発明の実施例1による他の鍵生成・選択装置*



【図14】



*のブロック図である。

【図4】本発明の実施例1～8による携帯型記憶装置のブロック図である。

【図5】本発明の実施例2による通信用端末のブロック図である。

【図6】本発明の実施例3による通信用端末のブロック図である。

【図7】本発明の実施例4による通信用端末のブロック図である。

【図8】本発明の実施例4による暗号装置のブロック図である。

【図9】本発明の実施例5による暗号装置のブロック図である。

【図10】本発明の実施例6による2乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図11】本発明の実施例6による鍵更新を行う場合の暗号通信を説明するための構成図である。

【図12】本発明の実施例7による通信用端末のブロック図である。

【図13】本発明の実施例8による2乗型疑似乱数を用いた鍵生成・選択装置のブロック図である。

【図14】共通鍵暗号通信ネットワークの構成図である。

【図15】公開鍵暗号通信ネットワークの構成図である。

【図16】共通鍵、公開鍵暗号通信ネットワークの構成図である。

【図17】従来の通信用端末のブロック図である。

【図18】DES暗号の1段分の処理を示すブロック図である。

【符号の説明】

10 通信端末

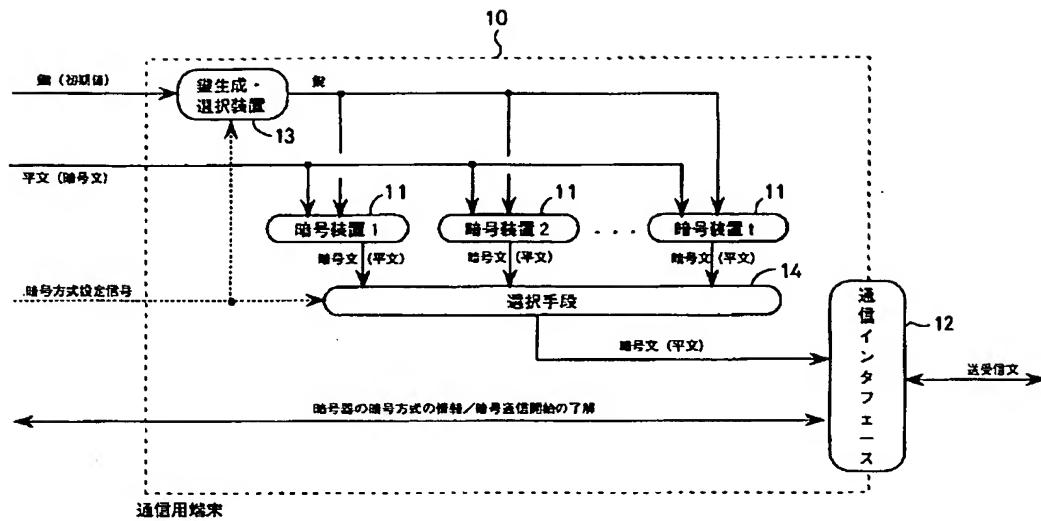
11～20 暗号装置

12 通信インターフェース

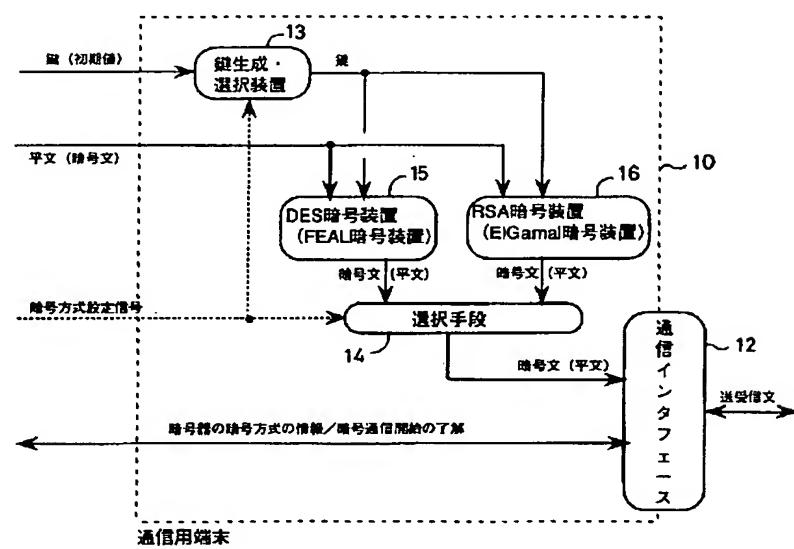
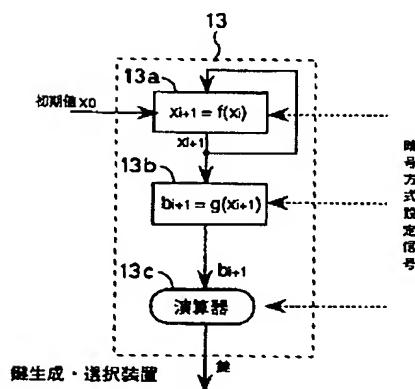
13 鍵生成・選択装置

14 選択手段

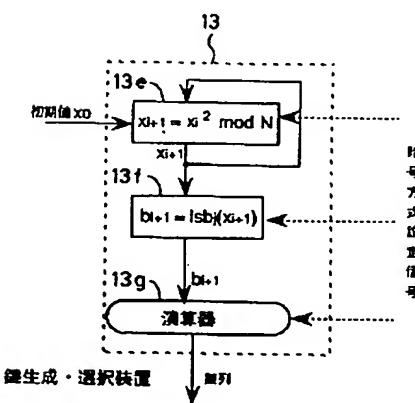
【図1】



【図2】

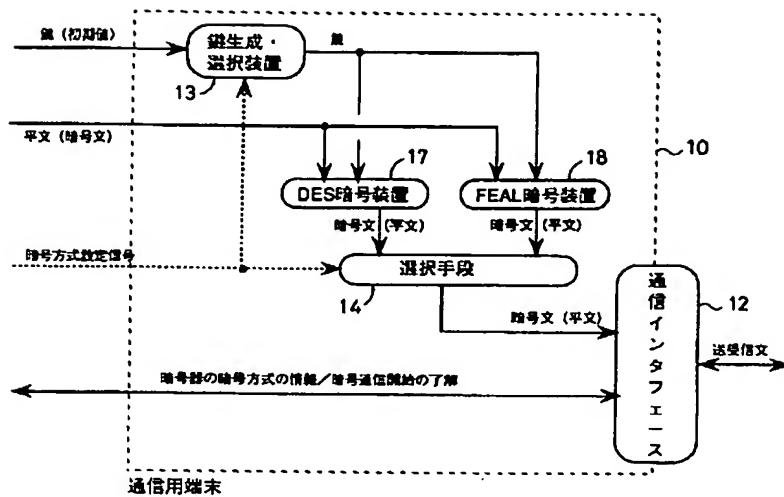


【図10】

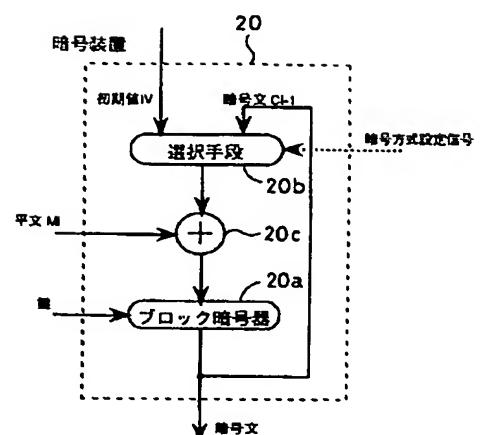


【図11】

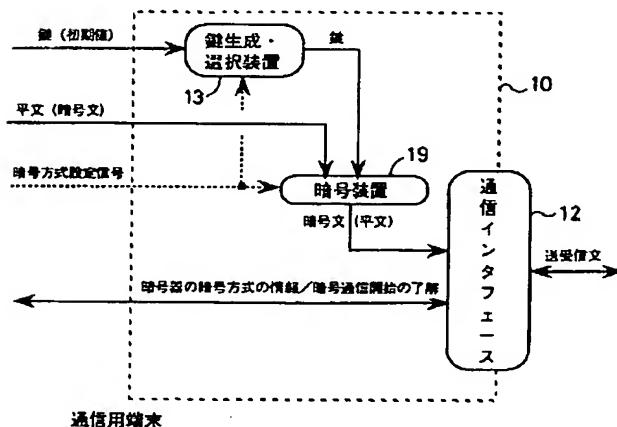
【図6】



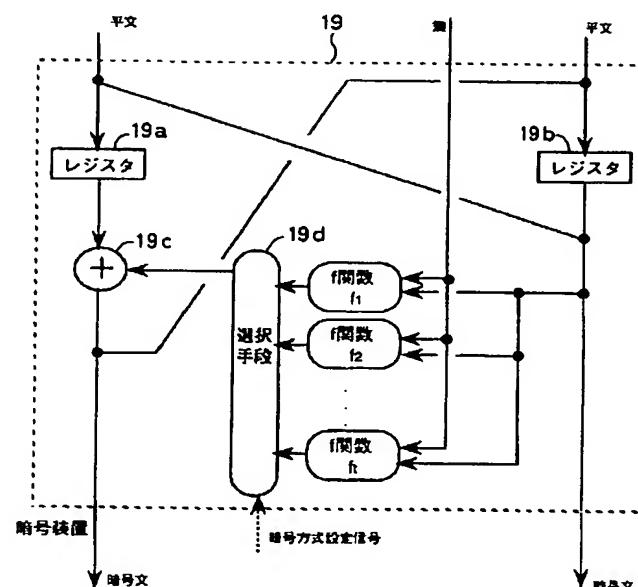
【図9】



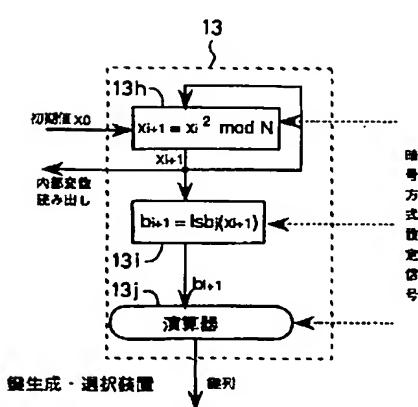
【図7】



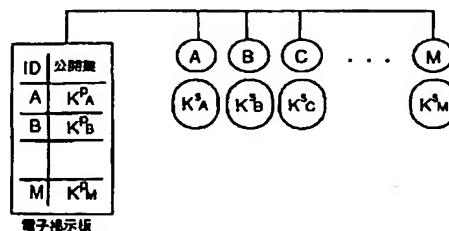
【図8】



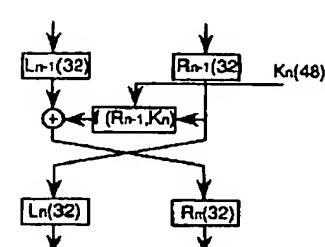
【図13】



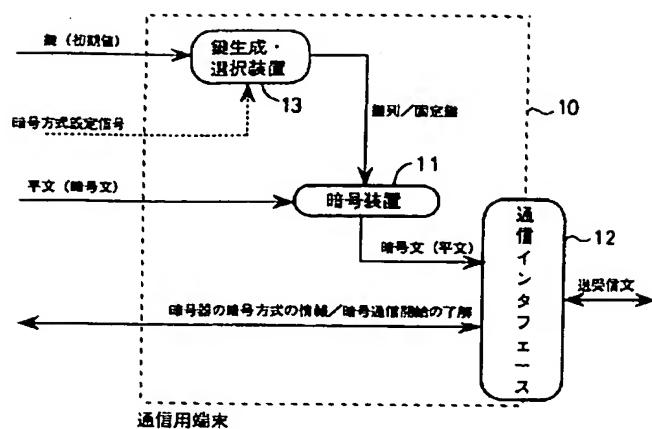
【図15】



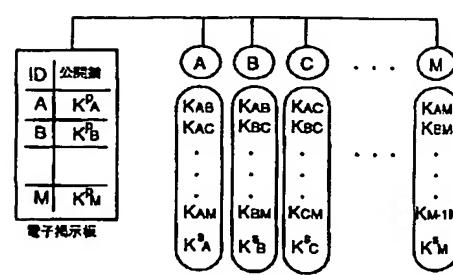
【図18】



【図12】



【図16】



【図17】

